Frequently Asked Questions about Alaska's 2016 Election

What actions has the Division of Elections taken to safeguard elections results?

DOE has protocols including a combination of people and technologies to ensure the security of eligible voters' ballots. The Division of Elections continues to work collaboratively with the State Office of Information Technology, National Association of Secretaries of State and the Department of Homeland Security on cyber security issues.

Since 2016, under the newly organized Office of Information Technology, the DOE has continued to work with the new agency to ensure that all aspects of our elections system remain secure. This partnership has allowed us to assess vulnerabilities by performing a variety of security tests, identify mitigation plans and share information on reports of threats or incidents. Collaborative work between election officials and state IT experts is just one of the methods continually used to ensure our voting systems remain secure.

Other protective measures include:

- Through the Election Infrastructure Program, DHS granted Elections Director secret security clearance which will allows access to timely and relevant threat information to Alaska election systems and infrastructure to ensure the best defenses are in place to protect those systems.

- Joining the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), which is a subsector of the Multi-State-ISAC. Through our membership, the division will gain access to an elections-focused cyber defense suite, including: sector-specific threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness and training products, and tools for implementing security best practices. As part of the EI-ISAC, we'll also have access to a 24x7x365 Security Operations Center, where we can reach out for assistance on a range of cybersecurity issues and needs.

- Continue to work collaboratively with State OIT on security enhancement projects which include tools to share secure information, monitor active attacks on our website and fortifying our security with elements of dual factor authentication.

- The Office of Information Technology (OIT) and the state's Chief Information Security Officer (CISO) are working closely with Elections to monitor the integrity of all systems

- OIT collaborates with a wide variety of Federal, State, local, Tribal, and other cyber partners to share cyber threat information

- OIT and Elections have increased cyber vigilance, reviewed existing practices, and are taking pro-active steps to mitigate potential risks

Were voting results altered by Russian actors or CyberZeist?
No, there is no evidence any result information was modified in any way.

Why wasn't the incident involving CyberZeist made public?
In communicating with the public, the Division attempts to use words that convey the truth as precisely as we can. We do this with the overarching goal of informing voters of any situation that would adversely impact the exercise of their voting rights. There are many adversaries seeking to subvert these rights, both domestic and foreign. In 2016 and now, we are actively working to prevent those adversaries from undermining voter confidence, especially as that is their stated goal.

Why does the division not describe these incidents as "compromises"?

The term "compromise" used by tech experts is conveyed in a technical sense of the word. In the non-technical sense, there was nothing to report as compromised since no element of the elections process was impeded by the event.

Did the hacker have capability to change voting results?
No, the division's results are not connected to the internet and the state does not have an online ballot tabulation system.

What did CyberZeist have the ability to do?
In this particular instance, the individual gained "read access" to our server which holds publicly available information. Nothing confidential was on this page.